REMARKS/ARGUMENTS

Claims Pending

Claims 1 to 38 are pending in this application. Claims 1, 15, 16, 17, 27, 34 and 36 are independent claims. Claims 2-14 are ultimately dependent from Claim 1, Claims 18-26 are ultimately dependent from Claim 17, Claim 35 is dependent from Claim 34, and Claims 37 and 38 are dependent from Claim 36. Claims 6, 7, 9, 10, 11, 21, 23 and 25 are amended to clarify the invention and correct typographical errors. Claims 8 and 22 are indicated as allowable if rewritten in independent form and Claims 7, 9 and 23-25 are indicated as allowable if rewritten to overcome rejections under 35 U.S.C. 112, second paragraph.

Applicant notes that no statutory basis is set forth for the rejection of Claims 27-38 and no detailed explanation of the rejection of Claims 27-38 is set forth in the Office Action. Also, Claims 27-33 are method claims, contrary to item 8 of the Office Action and no explanation of the rejection of Claim 27-33 is set forth in the Office Action.

Claims rejected under 35 U.S.C. § 112, second paragraph

Claims 7, 9, 11, 23, 25 and 31 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant notes that form paragraph 7.34.01 is not followed by any of form paragraph 7.34.02-7.34.15, a full explanation of the deficiency of the claims is not supplied for the rejections of Claims 7, 9, 23, 25 and 31, and the rejections of Claims 7, 9, 23, 25 and 31 are therefore unclear.

Applicant further submits when the definiteness of the claim language of Claims 7, 9, 23, 25 and 31 is analyzed "in light of:(A) The content of the particular

application disclosure;(B) The teachings of the prior art; and (C) The claim interpretation that would be given by one possessing the ordinary level of skill in the pertinent art at the time the invention was made," the rejected Claim language is clear and that the rejections of Claims 7, 9, 23, 25 and 31 should be withdrawn. The following remarks for individual claims are made in light of the limited information provided for each rejection.

Claim 7 is amended to delete "and user terminated." Claim 7 was rejected, stating that the phrase (sub step) "providing user initiated ~~and user terminated~~ connections to said user," is unclear. User initiated connections are known. By way of example, and not as a limitation, a dial-up telephone connection to a network is a user-initiated connection. Provision of user-initiated connections to a user is described at page 12, lines 9-23, of the present application. The phase "providing user initiated ~~and user terminated~~ connections to said user," is clear and the rejection of Claim 7 under 35 U.S.C. 112 should be withdrawn.

Claim 9 is amended to match the language of the written description at page 12, lines 24-36. In Claim 9 "a data quantity the is" is deleted, "bits" is rewritten as bytes, and "data quantity" is rewritten as "number of bytes of communication." Claim 9, as amended, is clear and the rejection of Claim 9 under 35 U.S.C. 112 should be withdrawn.

Claims 10 and 11 are amended to rewrite "service" as "product". A "product" may include "goods." The scope of products that may be provided under the present invention is described at page 15, lines 10-16, of the present application. Claim 11, as amended, is clear and the rejection of Claim 11 under 35 U.S.C. 112 should be withdrawn.

Claim 23 was rejected, stating that "anonymous Internet access" is unclear. "Anonymous" means of unknown name or identity. "Anonymous Internet access" using the present invention is described on page 30, lines 1-16, of the present application. Claim 23 is clear and the rejection of Claims 23 and 24 under 35 U.S.C. 112 should be withdrawn.

Claim 25 was rejected, stating that "anonymous email" is unclear. Email is described at page 18 to page 21, line 9, of the present application with page 20, lines 8 to 26, particularly addressing anonymous email. Anonymous email means that the user can anonymously send email or anonymously receive email or both.

Claim 25 is clear and the rejection of Claim 25 under 35 U.S.C. 112 should be withdrawn.

Claim 31 was rejected, stating that "preselected data" is unclear. The "preselected data" is described at page 13, lines 11 to 20, of the present application. Claim 31 is clear and the rejection of Claims 31, 32 and 33 under 35 U.S.C. 112 should be withdrawn.

Claims rejected under 35 U.S.C. § 102(b)

Claims 1, 10-14, 16-18, 20, 21 and 26 were rejected under 35 U.S.C. 102(b) as anticipated by U.S. Patent No. 6,029.150 to Kravitz. Claims 1, 10-14, 16-18, 20, 21 and 26 are believed to patentably define apparatus and methods not anticipated by Kravitz for the reasons hereafter set forth.

Briefly stated, in accordance with the present invention as claimed in Claim 1, there is claimed a method for conducting private secure electronic commerce comprising the steps of: providing first and second sequences of encryption key material, associating a value parameter with the first sequence, providing the first sequence to an anonymous user in exchange for a payment, providing encrypted data communications to the user until the value parameter is exhausted, and adjusting the value parameter in response to the step of providing encrypted data communications. The first sequence is suited for decrypting a message that has been encrypted using the second sequence, and the second sequence is suited for decrypting a message that has been encrypted using the first sequence.

Kravitz does not disclose providing first and second sequences of encryption key material as defined on page 10, lines 13 to 22 of the present application. Kravitz does not disclose sequences of continuous encryption material as in a one-time pad, sequences of identical session keys, or sequences of complimentary public and private keys. Kravitz specifically does not disclose providing first and second sequences of encryption key material at col. 8, lines 20-35, as stated in the Office Action. Kravitz does not disclose that the cryptographic keys mentioned at col. 22, lines 52-54 are sequential.

Kravitz does not disclose associating a value parameter with any first sequence. Kravitz specifically does not disclose associating a value parameter with the first sequence at col. 7, lines 45-55, as stated in the Office Action. Kravitz does not disclose that the encryption material has any value.

Kravitz does not disclose providing the first sequence to an anonymous user or providing the first sequence in exchange for a payment. In Kravitz the customer subscribes to a service and establishes an account, and the customer's bank and the CTA negotiate the availability of funds, so the customer/user is not anonymous. (Col. 12 lines 34-45.) Kravitz discloses using DSA signature in transactions to verify the identity of the customer, so the user in Kravitz is not anonymous. Kravitz discloses that the account must be funded before purchases can be made, but does not disclose that account funding is required before customer account is set up or the cryptographic keys mentioned at col. 22, lines 52-54, are provided to the customer. Kravitz does not disclose that account funding is a payment in exchange for anything, but rather discloses that account funding is for future payments to merchants in exchange for goods and services from the merchants.

Since Kravitz does not disclose providing first and second sequences of encryption key material, associating a value parameter with the first sequence, providing the first sequence to an anonymous user or providing the first sequence in exchange for a payment, Kravitz does not disclose all of the steps and limitations of Claim 1 and does not anticipate Claim 1.

Claim 10 is dependent from Claim 1, including all of the steps and limitations of Claim 1, and Claim 11 is dependent from Claim 10, so Kravitz does not disclose all of the steps and limitations of Claim 10 or 11 and does not anticipate Claim 10 or 11.

Claim 12 is dependent from Claim 1, including all of the steps and limitations of Claim 1, and further includes the step of providing anonymous network access to the user. Kravitz does not disclose providing anonymous network access to the user. In Kravitz, the identity of the customer is known to the CTA and generally to the merchant. The encryption schemes and account set ups disclosed in Kravitz require that the identity of the customer be known. The Office Action statement that implies that "anonymous" is synonymous with "encrypted communications is error." The DSA signature encryption and the public-private key encryption disclosed in Kravitz require that the identity of the customer be known, and are used to prove identity, not hide identity. Kravitz does not disclose all of the steps and limitations of Claim 1 or the further steps and limitations of Claim 12, and therefore does not anticipate Claim 12.

Claim 13 is dependent from Claim 1, including all of the steps and limitations of Claim 1, so Kravitz does not disclose all of the steps and limitations of Claim 13 and does not anticipate Claim 13.

Claim 14 is dependent from Claim 1, including all of the steps and limitations of Claim 1, and further claiming that the step of providing encrypted data communications includes the sub-steps of: generating a response to the user, encrypting the response by use of the second sequence into an encrypted response, sending the encrypted response to the user, and adjusting the value parameter in response to the step of sending. Kravitz does not disclose providing a second sequence and therefore does not disclose using a second sequence to encrypt a response. Kravitz does not disclose adjusting a value parameter in response to sending a response to a user. Since Kravitz does not disclose all of the steps and limitations of Claim 1 and does not disclose all of the further steps and limitations of Claim 14, Kravitz does not anticipate Claim 14.

Briefly stated, in accordance with the present invention, as claimed in Claim 16, there is claimed a method for conducting private secure electronic commerce comprising the steps of: providing first and second sequences of encryption key material, associating a value parameter with the first sequence, providing the first sequence to an anonymous user in exchange for a monetary payment proportional to the value parameter, providing encrypted application services to the user, providing anonymous network access to the user, adjusting the value parameter in response to the steps of providing encrypted application services and providing anonymous network access, and ceasing the providing encrypted application services and the providing anonymous network access when the value parameter is exhausted. The first sequence is suited for decrypting data that has been encrypted using the second sequence and the second sequence is suited for decrypting data that has been encrypted using the first sequence.

Kravitz does not disclose providing first and second sequences of encryption key material, associating a value parameter with the first sequence, providing the first sequence to an anonymous user, providing the first sequence in exchange for a payment, a payment proportional to the value parameter, or providing anonymous network access, as set forth in detail above. Kravitz does not include all of the steps and limitations of Claim 16 and does not anticipate Claim 16.

Briefly stated, in accordance with the present invention, as claimed in Claim 17, there is claimed a method for conducting private secure electronic commerce comprising the steps of: providing a first server, providing to an anonymous first user, in exchange for a payment, a first sequence of encryption key material, an identifier associated with said first sequence, connection instructions for connecting to the server, and encryption instructions for encrypting and decrypting data using the first sequence, providing to the server the identifier and a second sequence of encryption key material suitable for decrypting data that is encrypted with the first sequence and for encrypting data that can be decrypted with the first sequence, and providing encrypted data communications between the first user and the first server.

Kravitz does not disclose providing first and second sequences of encryption key material, providing the first sequence to an anonymous first user, or providing the first sequence in exchange for a payment, as set forth in detail above. Kravitz does not include all of the steps and limitations of Claim 17 and does not anticipate Claim 17.

Claims 18, 20 and 26 are dependent from Claim 17, and Claim 21 is dependent from Claim 20, each including all of the steps and limitations of Claim 17 and further steps and/or limitations. Since Kravitz does not anticipate Claim 17, Kravitz does not anticipate Claims 18, 20, 21 and 26. Claim 26 claims that the step of providing to an anonymous first user includes providing a portable data storage device suitable for access by a data processing device to the first user, the storage device including the first sequence of encryption key material and the identifier as stored data, and the connection instructions and the encryption instructions as executable software. Kravitz states at col. 22 line 50 to col. 23 line 20, that the public key is provided separate from the diskette with customer network software, and further that the software generates a public/private key pair for digital signature verification. Kravitz does not disclose providing a first sequence of encryption key material, or any encryption key material on the storage device.

Since Kravitz does not anticipate any of Claims 1, 10-14, 16-18, 20, 21 and 26, the rejections of Claims 1, 10-14, 16-18, 20, 21 and 26 under 35 U.S.C. 102 should be withdrawn.

Claims 27-33 are pending in the present application and no explanation of the rejection of Claims 27-33 was made in the Office Action. Claims 27-33 are addressed hereinafter in relation to Kravitz.

Briefly stated, Claim 27 claims a method of conducting secured electronic commerce through a server by a first user and the server, utilizing first and second sequences of encryption key material defining a pair of sequences in which each sequence of the pair is suited for decrypting data that has been encrypted using the other code sequence of the pair, comprising: providing to the first user the first sequence, providing to the encryption server the second sequence, establishing an account accessible to the server, wherein the account tracks a value parameter associated with use of the encryption key material of at least the first sequence, creating a first message by the first user, encrypting the first message by use of the first sequence, transmitting the encrypted first message by electronic means to the server, decrypting at least a portion of the encrypted first message at the server by use of the second sequence, accessing the account, adjusting the value parameter of the account in response to use of the encryption key material of at least the first sequence.

Kravitz does not disclose utilizing first and second sequences of encryption key material, providing the first sequence to a first user, providing the second sequence to the server, establishing an account that tracks a value parameter associated with the use of the encryption material of at least the first sequence or adjusting the value parameter in response to use of the encryption material of at least the first sequence. Kravitz does not include all of the steps and limitations of Claim 27 and does not anticipate Claim 27, or Claims 28-33, which are ultimately dependent from Claim 27.

Claims 34-38 are pending in the present application and the explanation of the rejection of Claims 34-38 made the Office Action is unclear. Claims 34-38 are addressed hereinafter in relation to Kravitz. Claim 34 claims apparatus for conducting secured electronic commerce comprising: a portable data storage device with stored data including a first sequence of encryption key material, and encryption software operable to encrypt and decrypt data by using the first sequence, a server having a second sequence of encryption key material suitable for decrypting data that has been encrypted using the first sequence and encrypting data such that the data can be decrypted with the first sequence, and a data processing device operable to connect to the portable data storage device, to access the stored data of portable data storage device, to execute the encryption software to encrypt and decrypt data by using the first sequence, to transmit data encrypted by using the first sequence to the server and to receive data encrypted by using the second sequence from the server.

Kravitz does not disclose a portable data storage device with stored data including a first sequence of encryption key material. Kravitz does not disclose a

server having a second sequence of encryption key material. Kravitz does not disclose all of the elements and limitations of Claim 34, or Claim 35, which is dependent from Claim 34, and therefore, Kravitz does not anticipate Claim 34 or Claim 35.

Claim 36 claims a portable data storage device, suitable for operation with a data processing device, with stored data for conducting secured electronic commerce, comprising: a first sequence of encryption key material suitable for decrypting data that has been encrypted by using a second sequence on a server and encrypting data such that the encrypted data can be decrypted by the server by using the second sequence, encryption software suitable for execution by the data processing device to encrypt and decrypt data by using the first sequence, an identifier associated with the first sequence for identifying the portable data storage device to the server, and connection software suitable for execution by the data processing device to connect the data processing device to the server for encrypted data communications therebetween.

Kravitz does not disclose a portable data storage device with a first sequence of encryption key material. Kravitz does not disclose a portable data storage device having the combination of encryption key material, encryption software, and an identifier for identifying the device and connection software. Kravitz does not disclose all of the elements and limitations of Claim 36, or Claims 37 and 38, which are dependent from Claim 36, and therefore, Kravitz does not anticipate Claim 36 or Claims 37 and 38.

Claims rejected under 35 U.S.C. § 103(a)

Claims 2-6, 15 and 19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kravitz in view of U.S. Patent No. 6,445,796 to Shefi. Claims 2-6 are ultimately dependent from Claim 1, Claim 15 is an independent claim, and Claim 19 is dependent from Claim 18, which is dependent from independent Claim 17.

Claim 2 includes all of the steps and limitations of Claim 1, and further claims that the first and second sequences are identical one-time pads. Kravitz does not teach or suggest providing first and second sequences of encryption key material, associating a value parameter with the first sequence, providing the first sequence to an anonymous user or providing the first sequence in exchange for a payment, as explained in detail above. Since Kravitz does not teach or suggest

associating a value parameter with the first sequence, Kravitz does not teach or suggest adjusting the value parameter in response to providing encrypted data communications. Kravitz also does not teach or suggest first and second sequences of identical one-time pads. Shefi does not teach or suggest associating a value parameter with the first sequence, providing the first sequence to an anonymous user, providing the first sequence in exchange for a payment or adjusting the value parameter in response to providing encrypted data communications. Since neither Kravitz nor Shefi nor their combination teach or suggest all of the steps and limitations of Claim 2, Claim 2 is not obvious from Kravitz in view of Shefi.

Claim 3 is dependent from Claim 2 and further claims adjusting the value parameter such that when the one time pad is exhausted, the value parameter is exhausted. The statement in the Office Action that Kravitz teaches the step of adjusting the value parameter such that when the one time pad is exhausted, the value parameter is exhausted, is error. Since Kravitz does not teach or suggest a one-time pad, Kravitz cannot teach or suggest simultaneous exhaustion of a value parameter of a one-time pad. Kravitz teaches funding of an account and payment independent of the quantity of encryption material. Shefi does not teach or suggest the deficiencies. Since neither Kravitz nor Shefi nor their combination teach or suggest all of the steps and limitations of Claim 3, Claim 3 is not obvious from Kravitz in view of Shefi.

Claim 4 is dependent from Claim 1 and further claims that the first and second sequences include an identical plurality of sequentially arranged session keys. The examiner takes Official Notice of purported sameness between session keys and one-time pads. Applicant respectfully traverses the correctness of the Official Notice as applied to Claim 4, noting that the Official Notice is error. A one-time pad is used bit-for-bit or byte-for-byte to encrypt and decrypt, with no bit or byte being reused ever, while a session key is reused repeatedly to encrypt a message or throughout a session. The mechanism and algorithm for encrypting and decrypting with a one-time pad is different than with a session key. In view of this distinction, the Official Notice should be withdrawn.

Kravitz does not teach or suggest providing first and second sequences of encryption key material, associating a value parameter with the first sequence, providing the first sequence to an anonymous user, providing the first sequence in exchange for a payment or adjusting the value parameter in response to providing encrypted data communications. Kravitz also does not teach or suggest first and second sequences of an identical plurality of sequentially arranged session keys.

Shefi does not teach or suggest associating a value parameter with the first sequence, providing the first sequence to an anonymous user, providing the first sequence in exchange for a payment, adjusting the value parameter in response to providing encrypted data communications, or first and second sequences of an identical plurality of sequentially arranged session keys. Since Kravitz and Shefi combined do not teach or suggest all of the steps and limitations of Claim 4, Claim 4 is not obvious from Kravitz in view of Shefi.

Claim 5 is dependent from Claim 4 and further claims adjusting the value parameter such that when the plurality of session keys is exhausted, the value parameter is exhausted. The statement in the Office Action that Kravitz teaches the step of adjusting the value parameter such that when the plurality of session keys is exhausted, the value parameter is exhausted, is error. Since Kravitz does not teach or suggest a plurality of session keys, Kravitz cannot teach or suggest simultaneous exhaustion of a value parameter and a plurality of session keys. Kravitz teaches funding of an account and payment independent of the quantity of encryption material. Shefi does not teach or suggest the deficiencies. Since Kravitz and Shefi combined do not teach or suggest all of the steps and limitations of Claim 5, Claim 5 is not obvious from Kravitz in view of Shefi.

Claim 6 is dependent from Claim 5 and further claims that the step of providing encrypted data communications including providing user initiated connections to the user, with the user utilizing a new session key from the plurality of session keys of the first sequence each time the user initiates a connection. Kravitz and Shefi combined do not teach or suggest all of the steps and limitations of Claims 4 or 5, as set forth above, and further combined do not teach or suggest using a new session key each time the user initiates a connection. Specifically, Shefi, at col. 5, lines 40-55, teaches encrypting with a one-time pad, not a session key. Since Kravitz and Shefi combined do not teach or suggest all of the steps and limitations of Claim 6, Claim 6 is not obvious from Kravitz in view of Shefi.

Briefly stated, Claim 15 claims a method for conducting private secure electronic commerce comprising the steps of: providing identical one-time pad first and second sequences of encryption key material, providing the first sequence to an anonymous user in exchange for a payment, receiving a message encrypted by use of the first sequence from the said user, decrypting at least a portion of the message by use of the second sequence, generating a response to the user, encrypting the response by use of the second sequence into an encrypted response, sending the encrypted

response to the user, and ceasing the sending and receiving when the first and second sequences have been completely used once.

Kravitz does not teach or suggest providing first and second sequences of encryption key material, providing one time pad first and second sequences, providing the first sequence to an anonymous user, providing the first sequence in exchange for a payment or ceasing the sending and receiving when the first and second sequences have been completely used once. Shefi does not teach or suggest providing the first sequence to an anonymous user, providing the first sequence in exchange for a payment or ceasing the sending and receiving when the first and second sequences have been completely used once. Since Kravitz and Shefi combined do not teach or suggest all of the steps and limitations of Claim 15, Claim 15 is not obvious from Kravitz in view of Shefi.

Claim 19 is dependent from Claim 18, which is dependent from Claim 17, and claims further steps and limitations. Kravitz does not teach or suggest providing first and second sequences of encryption key material, providing the first sequence to an anonymous first user, or providing the first sequence in exchange for a payment, as explained above for Claims 17 and 18. Shefi does not teach or suggest providing the first sequence to an anonymous first user, nor providing the first sequence in exchange for a payment. Since Kravitz and Shefi combined do not teach or suggest all of the steps and limitations of Claim 19, Claim 19 is not obvious from Kravitz in view of Shefi.

The rejections of 2-6, 15 and 19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kravitz in view of to Shefi should be withdrawn.

With regard to Claims 27-38, Kravitz does not teach or suggest all of the steps and limitations of method Claims 27-33 nor all of the elements and limitations of Claims 34-38, as explained above under the remarks for the 35 U.S.C. 102(b) rejections. Shefi does not teach or suggest the deficiencies of Kravitz. Claims 27-38 are not obvious from Kravitz in view of Shefi, and the rejection of Claims 27-38 should be withdrawn.

Conclusion

Reconsideration and allowance of Claims 1-38 is respectfully requested in view of the amendments and the foregoing remarks. Should any issues remain that

would preclude prompt allowance of this application, it is requested that the Examiner contact the undersigned attorney by telephone.

Attached is a request for Extension of Time of Two Months. A check in the amount of $210.00 for the extension of time is enclosed. If there is any discrepancy in the fee, please charge Deposit Account No. 06-0788.

Respectfully submitted,

Kyle W. Rost, Reg. No. 27943
Attorney for Applicant

5490 S. Autumn Court
Greenwood Village, CO 80111-3417
Telephone 720-528-8863
Facsimile 720-528-8864
Email rost@usa.net